IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

DAVID L. WOOD ET AL.

Serial No.: 09/357,726

Filed: July 21, 1999

For: SECURE DATA BROKER

Attorney Docket No.: SUNM 3633 PUS

Group Art Unit: 2131

Examiner: Aravind K. Moorthy

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief from the final rejection of claims 10-12, 17-26, 30-35 and 38-59 of the Office Action mailed on July 25, 2007 for the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is Sun Microsystems, Inc. ("Assignee"), a corporation organized and existing under the laws of the state of Delaware, and having a place of business at 4150 Network Circle, Santa Clara, California 95054, as set forth in the assignment recorded in the U.S. Patent and Trademark Office at Reel 012237/Frame 0134.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to the Appellants, the Appellants' legal representative, or the Assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 10-12, 17-26, 30-35 and 38-59 are pending. Claims 10-12, 17-26, 30-35 and 38-59 are rejected and are the subject of this appeal. Claims 1-9, 13-16, 27-29, 36 and 37 have been cancelled.

IV. STATUS OF AMENDMENTS

None.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 17 provides, in a networked computing environment, a method of securing access to an information resource behind a security barrier. The method includes predefining a request message specification corresponding to a structured request language, p. 7, l. 23 - p. 8, l. 9, formatting an access request in accordance with the structured request language, p. 7, l. 23 - p. 8, l. 9, and supplying the formatted access request to a first intermediary, the intermediary validating the formatted access request in accordance with the request message specification, p. 8, l. 11 - p. 9, l. 20. The method also includes forwarding the validated access request across the security barrier, p. 9, ll 20-24.

Claim 22 provides, in a networked computing environment, a method of securing access to an information resource behind a security barrier. The method includes predefining a response message specification corresponding to a structured response language, p. 10, l. 24 - p. 11, l. 2, formatting a response to an access request targeting the information resource, the formatted response being in accordance with the structured response language, p. 10, l. 24 - p. 11, l. 2, and supplying the formatted response to an intermediary, the intermediary validating the formatted response in accordance with the response message specification, p. 11, ll. 2-18. The method also includes forwarding a validated response across the security barrier, p. 11, l. 19-23.

Claim 24 provides an information security system. The system includes a security barrier, Fig. 1, 140, a proxy, Fig. 1, 111, for an information resource, Fig. 1, 180, the proxy and the information resource on opposing first and second sides, respectively, of the security barrier, Fig. 1. The system also includes a data broker, Fig. 1, 120, on the first side of the security barrier, wherein, in response to an access request targeting the information resource, the data broker validates a request message encoded in a structured request language against a predefined request message specification therefor and forwards only validated request messages across the security barrier, p. 8, l. 11 - p. 9, l. 24.

Claim 30 provides a computer program product encoded in computer readable media. The computer program product includes data broker code and parser code executable on a first network server separated from an information resource by a security barrier, p. 8, l. 11 - p. 9 - l. 25. The data broker code includes instructions executable as a first instance thereof to receive access requests in a structured language corresponding to a predefined request message specification and to forward validated ones of the access requests across the security barrier toward the information resource, p. 8, l. 11 - p. 9 - l. 25. The parser code includes instructions executable as a first instance thereof to validate the received access requests against the predefined request message specification, p. 8, l. 11 - p. 9 - l. 25.

Claim 42 provides a method of securing a data transaction across a security barrier. The method includes validating a request message encoded in a structured request language against a predefined request message specification therefor, p. 7, l. 23 - p. 9, l. 20, and transmitting the validated request message across the security barrier, p. 9, ll. 20-24. The method also includes validating a response message encoded in a structured response language against a predefined response message specification therefor, the response message corresponding to the validated request, p. 10, l. 24 - p. 11, l. 18, and transmitting the validated response message across the security barrier, p. 11, ll. 19-23.

Claim 55 provides, in a networked information environment including a client and an information resource separated by a security barrier, an information security system. The system includes means for proxying an access request by the client targeting the information resource and for preparing a request message corresponding to the access request in a structured language corresponding to a predefined request message specification. P. 7, l. 23 - p. 8, l. 9. The system also includes means for validating the request message against the predefined request message specification and forwarding only validated request messages across the security barrier. P. 8, l. 11 - p. 9, l. 24.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 10, 17-26, 30, 31, 34, 35, 42, 43, 45-47, 51 and 53-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Dixon (US Pat. No. 6,289,461). Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dixon in view of Ottensooser (US Pat. No. 5,905,856). Claims 32, 33, 38-41, 48-50, 52, 58 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dixon in view of Bobo (US Pat. No. 5,870,549). Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dixon in view of Schneier (Applied Cryptography).

VII. ARGUMENT

A. Claims 10, 17-26, 30, 31, 34, 35, 42, 43, 45-47, 51 and 53-57 are patentable under 35 U.S.C. 102(e) over Dixon

With regard to claims 17, 22, 24, 30, 42 and 55, the Examiner attempts to find all the claimed limitations in the following passages of Dixon:

> FIG. 4 illustrates one embodiment of an HTTP request in more detail. An HTTP request includes header information which identifies it as an HTTP request, specifies the destination of the request, and specifies various additional characteristics. The header can be followed by data in any format. In the illustrated

embodiment, the data includes a prefix indicating which messages, if any, client system 110 received in the last response from server system 120. Here, the prefix indicates that client system 110 received messages 1 through N in the last response. After the prefix, the request also includes copies of all the messages 1 through M stored in buffer 220. When the request is received by server system 120, server system 120 will provide messages 1 through M to server process 310. Server system 120 will also remove messages 1 through N from the messages stored in buffer 320 and send only the remaining messages, if any, in the next response.

FIG. 5 illustrates one embodiment of an HTTP response. Like the request, the response includes header information which identifies it as an HTTP response corresponding to a particular HTTP request, specifies the destination, and specifies various additional characteristics of the response. The header can be followed by data in any format. In the illustrated embodiment, the data includes a prefix indicating which messages, if any, server system 120 received in the last request. Here, the prefix indicates that server system 120 received messages 1 through M in the last request. After the prefix, the response also includes copies of the messages 1 through N stored in buffer 320. When the response is received by client system 110, client system 110 will provide messages 1 through N to client process 210, remove messages 1 through M from the messages stored in buffer 220, and send only the remaining messages, if any, in the next request.

Neither system removes a message from its buffer before receiving an indication that the message was received. Also, as discussed above, client system 110 will send a request if a response is not received within a certain amount of time. For example, if a request never reaches server system 120 for whatever reason, client system 110 will send another request including the same messages and any additional messages that may have accumulated. Similarly, if a response never arrives, client system 110 will send another request and server system 120 will send another response including the same messages and any additional messages that may have accumulated. Furthermore, if a request or a response is received, but the messages are unreadable, the corresponding returned prefix will

> indicate that the messages were unreadable and the messages will be resent. In this manner, the present invention provides reliable message transmission over inherently unreliable communications media.
>
> Col. 6, l. 43 - col. 7, l. 27.

The above merely discusses the format of HTTP requests/responses and indicates that client system 110 and server system 120 issue these requests/responses respectively. The above also discusses the mechanism by which Dixon provides reliable message transmission. The above, however, does not teach all the elements of claims 17, 22, 24, 30, 42 and 55.

> The Examiner asserts that
>
> Dixon discloses that HTTP transactions can only be initiated by client systems; firewall 140 can be designed to only allow out-going HTTP requests and only allow in-coming HTTP responses that correspond to the out-going requests. Therefore, the firewall only allows HTTP (outgoing and incoming) messages. The message specification is HTTP. The security barrier is firewall 140.
>
> Office Action, July 25, 2007, pp. 2-3.

These assertions, however, lack technical merit for the reasons explained below.

With regard to claim 17, Dixon does not teach predefining a request message specification corresponding to a structured request language or formatting an access request in accordance with the structured request language. The Examiner asserts that the "message specification is HTTP." Office Action, July 25, 2007, p. 3. HTTP, however, does not correspond to a structured request language, such as XML, because HTTP can be used to tunnel any information through a firewall. As such, HTTP allows arbitrary byte streams to be sent as a request and returned as a response.

With regard to claim 17, Dixon does not teach supplying the formatted access request to a first intermediary, the intermediary validating the formatted access request in accordance with the request message specification. Dixon simply lacks the claimed intermediary. The firewall of Dixon validates transport protocols, not formatted access requests in accordance with request message specifications.

With regard to claim 22, Dixon does not teach predefining a response message specification corresponding to a structured response language or formatting a response to an access request targeting the information resource, the formatted response being in accordance with the structured response language. As explained above, HTTP does not correspond to a structured response language.

With regard to claim 22, Dixon does not teach supplying the formatted response to an intermediary, the intermediary validating the formatted response in accordance with the response message specification. As explained above, Dixon simply lacks the claimed intermediary.

With regard to claim 24, Dixon does not teach a data broker on the first side of the security barrier, wherein, in response to an access request targeting the information resource, the data broker validates a request message encoded in a structured request language against a predefined request message specification therefor. As explained above, HTTP does not correspond to a structured request language and Dixon simply lacks the claimed data broker.

With regard to claim 30, Dixon does not teach data broker code including instructions executable as a first instance thereof to receive access requests in a structured language corresponding to a predefined request message specification. As explained above,

HTTP does not correspond to a structured language and Dixon simply lacks the claimed data broker code.

With regard to claim 42, Dixon does not teach validating a request message encoded in a structured request language against a predefined request message specification therefor. As explained above, HTTP does not correspond to a structured request language and the firewall of Dixon validates transport protocols, not request messages encoded in a structured request language against a predefined request message specification.

With regard to claim 42, Dixon does not teach validating a response message encoded in a structured response language against a predefined response message specification therefor, the response message corresponding to the validated request. As explained above, HTTP does not correspond to a structured response language and the firewall of Dixon validates transport protocols, not response messages encoded in a structured response language against a predefined response message specification.

With regard to claim 55, Dixon does not teach means for proxying an access request by the client targeting the information resource and for preparing a request message corresponding to the access request in a structured language corresponding to a predefined request message specification. As explained above, HTTP does not correspond to a structured language.

With regard to claim 55, Dixon does not teach means for validating the request message against the predefined request message specification and forwarding only validated request messages across the security barrier. As explained above, the firewall of Dixon validates transport protocols, not request messages against predefined request message specifications.

Claims 10, 18-21, 23, 25, 26, 31, 34, 35, 43, 45-47, 51, 53, 54, 56 and 57 are patentable because they depend from one of the independent claims.

B. Claims 11 and 12 are patentable under 35 U.S.C. 103(a) over Dixon in view of Ottensooser

Claims 11 and 12 are patentable for the reasons claim 42 is patentable.

C. Claims 32, 33, 38-41, 48-50, 52, 58 and 59 are patentable under 35 U.S.C. 103(a) over Dixon in view of Bobo

Claims 32, 33, 38-41, 48-50, 52, 58 and 59 are patentable because they depend from one of the independent claims.

D. Claim 44 is patentable under 35 U.S.C. 103(a) over Dixon in view of Schneier

Claim 44 is patentable for the reasons claims 42 is patentable.

The fee of $510 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) is enclosed. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

Respectfully submitted,

DAVID L. WOOD ET AL.

By: /Benjamin C. Stasa/
Benjamin C. Stasa
Registration No. 55,644
Attorney for Applicants

Date: December 21, 2007

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351; Enclosure - Appendices

VIII. CLAIMS APPENDIX

10. A method as in claim 42 wherein the request and the response message validatings are respectively performed at first and second secure data brokers on opposing sides of the security barrier; and

wherein the validated request and response message transmissions are between the first and second secure data brokers.

11. A method as in claim 42 wherein the request message validating includes:

parsing the request message using Data type Definitions (DTDs) encoding a hierarchy of valid tag-value pairs in accordance with syntax of a valid request message; and

if the request message is not successfully parsed, forwarding a response message without transmission of the request message across the security barrier.

12. A method as in claim 42

wherein the response message validating includes:

parsing the response message using Data Type Definitions (DTDs) encoding a hierarchy of tag-value pairs in accordance with syntax of a valid response message.

17. In a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

predefining a request message specification corresponding to a structured request language;

formatting an access request in accordance with the structured request language;

supplying the formatted access request to a first intermediary, the intermediary validating the formatted access request in accordance with the request message specification; and

forwarding the validated access request across the security barrier.

18. A method as in claim 17, further comprising:

accessing the information resource in accordance with the validated access request.

19. A method as in claim 17, further comprising:

receiving, at an application proxy, an access request targeting the information resource; and

performing the access request formatting at the application proxy.

20. A method as in claim 17, further comprising:

predefining a response message specification corresponding to a structured response language;

formatting a response to the access request in accordance with the structured language;

supplying the formatted response to a second intermediary, the second intermediary validating the formatted response in accordance with the response message specification; and

forwarding a validated response across the security barrier.

21. A method as in claim 20, further comprising:

accessing the information resource in accordance with an access request from a client; and

supplying the client with a response in accordance with the validated response.

22. In a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

predefining a response message specification corresponding to a structured response language;

formatting a response to an access request targeting the information resource, the formatted response being in accordance with the structured response language;

supplying the formatted response to an intermediary, the intermediary validating the formatted response in accordance with the response message specification; and

forwarding a validated response across the security barrier.

23. A method as in claim 22, further comprising:

accessing the information resource in accordance with the access request from a client;

supplying the client with a response in accordance with the validated response.

24. An information security system comprising:

a security barrier;

a proxy for an information resource, the proxy and the information resource on opposing first and second sides, respectively, of the security barrier;

a data broker on the first side of the security barrier, wherein, in response to an access request targeting the information resource, the data broker validates a request message encoded in a structured request language against a predefined request message specification therefor and forwards only validated request messages across the security barrier.

25. An information security system as in claim 24, further comprising:

a second data broker on the second side of the security barrier, wherein, in response to an access targeting the information resource, the second data broker validates a

response message against a predefined response message specification and forwards only validated response messages across the security barrier.

26. An information security system as in claim 24, further comprising:

the information resource.

30. A computer program product encoded in computer readable media, the computer program product comprising:

data broker code and parser code executable on a first network server separated from an information resource by a security barrier;

the data broker code including instructions executable as a first instance thereof to receive access requests in a structured language corresponding to a predefined request message specification and to forward validated ones of the access requests across the security barrier toward the information resource; and

the parser code including instructions executable as a first instance thereof to validate the received access requests against the predefined request message specification.

31. the computer program product of claim 30, further comprising:

an encoding of the predefined request message specification.

32. The computer program product of claim 30,

wherein the data broker code and parser code are also executable on a second network server separated from a client application by the security barrier;

wherein the data broker code includes instructions executable as a second instance thereof to receive responses in a structured language corresponding to a predefined response message specification and to forward validated ones of the responses across the security barrier toward the client application; and

wherein the parser code includes instructions executable as a second instance thereof to validate the received responses against the predefined response message specification.

33. The computer program product of claim 32, further comprising:

an encoding of the predefined response message specification.

34. The computer program product of claim 30, further comprising:

application proxy code including instructions executable to format the access requests in accordance with the structured language corresponding to the predefined request message specification.

35. The computer program product of claim 30, encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other

magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

38. the method of claim 17 wherein the structured request language includes a markup language.

39. The method of claim 38 wherein the markup language includes eXtensible markup language.

40. The information security system of claim 24 wherein the structured request language includes a markup language.

41. The information security system of claim 40 wherein the markup language includes eXtensible markup language.

42. A method of securing a data transaction across a security barrier, the method comprising:

validating a request message encoded in a structured request language against a predefined request message specification therefor;

transmitting the validated request message across the security barrier;

validating a response message encoded in a structured response language against a predefined response message specification therefor, the response message corresponding to the validated request; and

transmitting the validated response message across the security barrier.

43. A method as in claim 42,

wherein the request and response message specifications are predefined in accordance with the valid request and response message constraints specific to an information resource.

44. A method as in claim 42,

wherein at least one of the request and response message specifications is cryptographically secured.

45. A method as in claim 42, further comprising:

receiving, at an application proxy, an access request targeting an information resource;

formatting the request message in a structured language corresponding to the request message specification; and

transmitting the formatted request message to a secure data broker for the request message validating.

46. A method as in claim 42, further comprising:

formatting the response message in a structured language corresponding to the response message specification; and

transmitting the formatted response message to a secure data broker for the response message validating.

47. A method as in claim 42, further comprising:

accessing an information resource in accordance with the validated request message; and

preparing the response message in accordance with the access.

48. A method as in claim 47,

wherein the response message is formatted in a structured language corresponding to the response message specification.

49. A method as in claim 42,

wherein the request message is formatted in a structured language corresponding to the request message specification; and

wherein the response message is formatted in a structured language corresponding to the response message specification.

50. A method as in claim 49,

wherein the structured languages corresponding to the request and response message specifications include an eXtensible Markup Language (XML).

51. A method as in claim 42,

wherein at least one of the validated request message transmitting and the validated response message transmitting is via a secure protocol.

52. A method as in claim 42,

wherein at least one of the validated request message and the validated response message is encoded in a markup language.

53. A method as in claim 42,

wherein the security barrier includes a firewall.

54. A method as in claim 42,

wherein the security barrier includes a secure communication channel between servers.

55. In a networked information environment including a client and an information resource separated by a security barrier, an information security system comprising:

means for proxying an access request by the client targeting the information resource and for preparing a request message corresponding to the access request in a structured language corresponding to a predefined request message specification;

means for validating the request message against the predefined request message specification and forwarding only validated request messages across the security barrier.

56. An information security system as in claim 55, further comprising:

means for validating a response message against a predefined response message specification and forwarding only validated response messages across the security barrier.

57. An information security system as in claim 55, further comprising the security barrier.

58. The method of claim 42 wherein the structured request language comprises a markup language.

59. The method of claim 58 wherein the markup language comprises eXtensible markup language.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.